ISSN: 2278-4632
Vol-10 Issue-1 January 2020

CLASSIFICATION OF VARIOUS ATTACKSAND SECURITY ISSUES IN WIRELESS SENSOR NETWORK

Dr. Chinmay R. Pattanaik[1], Ms Smruti Mishra[2]*
*[1]*Associate Professor,Dept. Of Computer Science and Engineering, NIT , BBSR*
[2]Assistant Professor,Dept. Of Computer Science and Engineering, NIT , BBSR
chinmayaranjan@thenalanda.com, smrutimishra@thenalanda.com*

Abstract

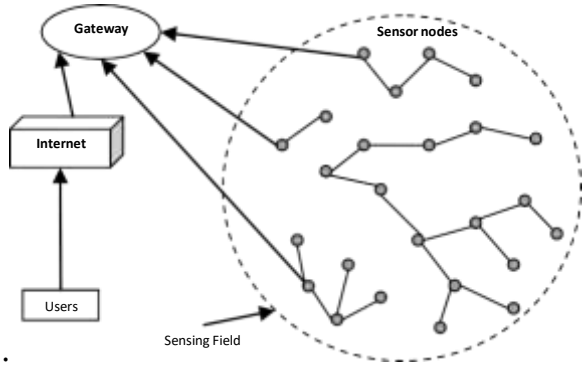
Wireless sensor networks (WSN) have a set of algorithms and protocols with self-establishing capabilities. These sensors work with each and every different to sense some bodily phenomenon after which the information gather is processed to get relevant outcomes. These sensor nodes can calculate, sense, and assemble particulars from the atmospheres and based totally on some nearby decision process, they are in a position to transmit the sensed files to the person. The battery is the foremost electrical energy grant in a sensor node and secondary energy supply that harvests energy from the atmospheres together with photo voltaic panels may additionally be brought to the node depending on the appropriateness of the atmospheres where the sensor will be diffuse. Clustering is the method which performs the grouping of similar nodes and then starts communicating into the clusters. Security can be finished by means of encrypting and decrypting the facts and make them unable to read that from the malicious users. Cryptography is the useful technique which contains symmetric and asymmetric methods. In this paper we find out about about WSN and its utility or a number of assaults which exist in the sensor community in the middle of paper we talk about a variety of existing technique and it's working. Various assaults are carried out in this community such as passive and lively assaults or insider and outsider attacks. The wirelessly network always required protection in the form of information integrity, confidentiality, authenticity and etc.

Keywords— WSN; attacks; security; security issues;

I. INTRODUCTION

A WSN involves of spatial allotted self-directed sensors to environment circumstances or display physical, e.g. sound, pressure, temperature, etc. [1]. These sensors are slight, and they are inexpensive and with restrained processing and computing assets as equaled to fashionable sensors. These sensor nodes can measure, sense, and accumulate information from the atmospheres and, primarily based on some local decision process, they are succesful to transfer the sensed archives to the person. Sensor nodes are lowest energy device ready with one or greater sensors, a processor, memory, a energy supply, a radio, and an actuator.

A variety of thermal, organic, optical, mechanical, and magnetic and chemical sensors can be linked to the sensor node tomeasure belongings of the atmosphere. Since the sensor nodes have limited reminiscence and are usually diffuse in the difficult-to-get entry to places, a radio is carried out for wirelessly communiqué to transfer the documents to a base station (BS) (e.g., a computer, a non-public handheld device, ora get proper of entry to aspect to a set infrastructure). Battery is the important electricity provide in a sensor node. Secondary power furnish that harvests electricity from the atmospheres collectively with solar panels might also be add to the node relying on the appropriateness of the atmospheres the place the sensor will be diffuse. Depend on the utilization and the variety of sensors utilized; actuators may additionally be integrated in the sensors



[2].

II. WSN APPLICATION

We can categorize the tradition of WSN into defense applications, forest applications, as well as domestic applications.

A. Defense applications

WSNs can be an indispensable section of protection command, security control, records communications, computation, intelligence, concentrated on systems such as surveillance etc.

B. Forest applications

Certain environmentally utilization of sensor networks (SN) contain recording and notice the activities of minor birds and insects, monitoring environmental conditions, animals, earth monitoring and exploration.

C. Medical Science applications

Certain of the purposes of health for SN are diagnosing the patients, tracking region and motion of patients and medicalpractitioner inside health facility etc.

D. Industrial applications

Certain industrial functions of WSNs are make virtualkeyboards, environmental control in office constructions, robot control, interactive toys, monitoring product fantastic etc.

III. TYPE OF WSN

According to previously lookup art work accomplished five varieties of WSN are possible relying upon wherein and how sensors are hooked up up to reveal info. According to thesehomes of sensor deployment we are in a position to classify WSNs into five essential kinds namely; underground WSN, Ground (terrestrial) WSN, aquatic (underwater) WSN, and mobility WSNs.

A. Ground (Terrestrial) WSNs

Usually consist of hundreds to thousands of cheap WSN arranged randomly in a given sensing region. Sensor nodes canbe plunged from a randomly and plane situated into the target region in ad hoc diffuse. In a position (terrestrial) WSN, reliable communiqué in a intense atmosphere is very vital. Ground sensor nodes must be able to efficiently communicate info return to the BS. Whereas battery power is constrained resource aid and it's important restraint on network performance and its competent to not be rechargeable or replaceable again, ground sensor nodes yet can be well- found with a secondary power source e.g battery or solar cell. So due to this it is forever important for sensor nodes to preserve energy.

B. Underground WSNs

Underground WSNs are sequence of few of the sensor nodes placed inside the earth crust or in a cave or in a mine and they may be utilized to reveal underground things to do collectively with volcanic situations and many others. Extra sink or BS nodes are positioned above crust of earth to transmit info from the sensor nodes to the BS.These category of WSN are a entire more high cost than a ground (terrestrial) WSN in stages of equipment, maintenance and deployment. subversive sensor nodes are additional high priced because vital device parts ought to be decided on to ensure reliable communiqué thru soil, water, rocks, and other stuffing residing internal crust. The inside

ISSN: 2278-4632
Vol-10 Issue-1 January 2020

circumstances atmosphere produce wirelessly communiqué a challenge because of highest levels of signal losses andreduction.

C. Aquatic (Underwater) WSNs

Aquatic WSNs consist of few of sensor nodes and vehicles disperse under water. As conflicting to ground WSNs, aquatic sensor nodes are extra high-priced and lesser sensor nodes are disperse in sensing region. Self-directed aquatic vehicles are utilized for accumulating or exploration facts from sensor nodes. As in evaluation to a dense diffuse of sensor nodes in a floor WSN, a sparse diffuse of sensor nodes is positioned at sea level. Typical aquatic (underwater) wirelessly communications are applied thru transmission of acoustic waves.

D.Multi-media WSNs

Multi-media WSNs are mixture of a no. of lowest charge sensor nodes well-appointed with microphones and cameras. These sensor nodes interconnected with each and every one of a kind over a wirelessly connection for information sensing, documents processing, records correlation, and records compression. Multi-media WSNs are utilized to allow monitoring of activities inside the form of multimedia programs.

E.Mobile WSNs

Mobility WSNs are a no. of transferring sensor with their interaction with sensing atmosphere. Moving sensor nodes have the viable to compute, like non-moving nodes. Mobility WSNs are utilized in navy and other industrial applications [3].

IV.ATTACKS ON WSN

A. Internal Attacks

These are mainly performed due to the fact of the compromised nodes. These compromised nodes always are searching for to disrupt or parallelize the network. Based on kind of undertaking performed by using attacker, it can be further classified as: Outside Attack- in which, an attacker can replace/introduce new malicious node from outside. Inside Attack- in which, an attackercan two seize any node; reprogram it, to act as malicious node.

B. External Attacks

In these attacks, the attacker node isn't forever an endorsed contribute of SN. Depend on the behavior of attacker node, it could be classified as:

- Passive Attack- it includes snoopping on or observing packets exchanged with WSN. It engages only unauthorizedlistening to the routing packets.
- Generally, encryption is the standard solution to preservebeside these attacks.

- A

ct
st
wrong stream. moreover, it results in unruly netw
attacks, Jamming attacks &Power Exhaustion

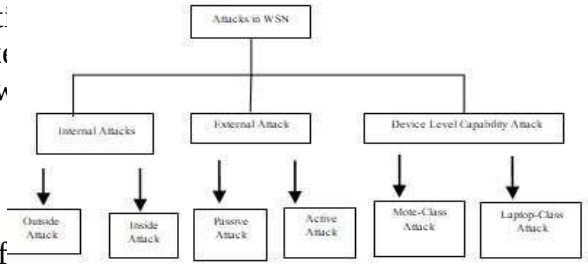


Fig. 2 Attack classifications in WSN

I. Device Level Capability Attack

This type of assaults is labeled depend on the f for attacking. An attacker may additionally assaul ine (Sensor Level) or more effective laptop computer machine (Laptop Level). An adversary can fairly injury the machine if he/she makes use of Laptop Class assault having extra effective computation, storage and battery life. Beside the above noted classifications, an attacker may utilize one or greater of the subsequent assault techniques.

J. Eavesdropping

ISSN: 2278-4632
Vol-10 Issue-1 January 2020

In which an attacker mutely listen to media for announcement amid two parties and don't adapt the data. It's a passive technique.

K. Radio jamming

In this attack, the attacker tries to disrupt the conversation by sending few radio waves at the comparable frequency resulting in interference or collisions of packets over network. Jamming can be intermittent or non-stop depend on the time for which community is kept jammed.

L. Message's injection

In this the attacker broadcasts many false messages above network in lieu of humiliating the packet data or to simply fatigue network.

M. Message's replication

In this the attackers imprison and resend the identical packet many times to similar or different sensor and at dissimilar times in succession to make receiver foolish.

N. Node compromise (Destruction or theft)

This includes physical capturing of a node in succession to interrupt network by flouting the communication alleyway or reprogramming a node so that it acts as a spy in network.

O. Denial of Service (DoS)

In this the attacker will frequently sends packet in succession to interrupt services or battery power through using malicious nodes. This is an vigorous type of attack.

P. HELLO Flooding

We recognize that HELLO message is used for discovering neighbors. In this structure of attack, the attacker makes use of extra effective nodes to ship HELLO messages to far away sensor nodes so that they believe that the malicious node is their neighbor and they will transfer future packets to it.

Black Hole Attack

In this attack a node attempts to become receiver of packets of adjacent nodes by altering their routing table and it will never ahead the packets to exact destination.

Q. Selective Forwarding (Gray Hole Attack)

in this attack, the attacker will insert node of malicious in the n/w which tries to alternate the routing and capture data just like black gap attack however unlike it will selectively forward facts (not all) and so difficult to detect.

R. Wormhole Attack

This kind of attack is carried out with at least two malicious nodes which have high bandwidth between them either wired or wirelessly. These malicious nodes will show different regular nodes that they furnish the shorter route to the goal even if they are lying far away in the network. So, the node will forward statistics to the malicious node that can be captured by means of attacker easily.

S. Sinkhole Attack

In this attack the malicious node exist in near the BS and it tries to fantasy to be contiguous node to the BS so that other neighboring usual node will change themselves and ahead info to the malicious node.

T. Sybil Attack

In this attack the adversary tries to have countless individualists to exclusive nodes and consequently can be in more than one region at single time. Here it tries to be voted as the cluster head. A Sybil assaults is enormous danger to Geographic Routing Protocols.

U. Infinite Loops-

In this assault two or extra malicious node tries to flow into packets infinitely in the n/w in sequence to exhaust electricity of the network.

V. Message Alteration

In this assault the node of malicious will detain and adjust packets on the network. It can add bogus data or remove data so that packet will turn into tainted.

W. Sleep deprivation torture

In this assault, the malicious node will avert a node from latent by sending messages to it or asks

ISSN: 2278-4632
Vol-10 Issue-1 January 2020

for estimation. This is absolute so that the node will devour its power rapidly [4].

V. SECURITY REQUIREMENTS IN WSN

A WSN is a distinct form of network. It shares few commonalities with a common laptop network, however also exhibitions many features that are sole to it. The offerings of protection have to be protecting the info communicated over the n/w and the sources from attacks and nodal misconduct in a WSN. The quintessential protection requirements are listed below:

A. Data confidentiality

The safety mechanism wants to make positive that no message in the n/w is understood with the useful resource of everybody barring supposed recipient. In a WSN, the complicated of confidentiality ought to tackle the next requirements.

B. Availability

This necessities make certain which the WSN offerings ought to be handy constantly even in prevalence of an external or interior assaults e.g. DoS. Dissimilar strategies have been described thru investigators to accomplish this objective. While some mechanisms create exploit of extra communiqué among nodes, others advocate utilize of a central get entry to manipulate system to make certain profitable transfer of all message to its receiver.

C. Data freshness

It implies which the information is cutting-edge and make sure which no opponent can replay old messages. This requirement is especially vast when the WSN nodes develop shared- keys for message communiqué, whereas a potential opponent can commence a repeat attack developing the old key as the latest key is being broadcasted to every the nodes in the WSN.A time- precise counter may be placed in to all packet to ensure the purity of the packet.

D. Self-organization

Every node in a WSN have to be self-organizing and self- recuperation. This characteristic of a WSN moreover poses good challenges to safety. The WSN dynamic nature makes it sporadically not possible to fixing any pre-installed shared key mechanism the numerous nodes and the BS. A no. of key pre- distribution scheme have been describe inside the context of symmetric encryption However, for software of public-key cryptographic methods an efficient mechanism for key distribution could be extremely a great deal vital. It's perfect that the nodes in a WSN self-establish between themselves no longer simplest for multi-hop routing though also to carryout key control and growing trust relations.

E. Secure localization

In many conditions, it will befall necessary to precisely and routinely determine each sensor node in a WSN. For example, a WSN intended to locate errors would require accurate localities of sensor nodes distinguish the faults. A capacity challenger can without complexity provide and influence false locality info with the help of reporting fake sign benefit, replaying messages and so on. If the info statistics isn't forever secured correctly. The writers in have distincted a way called as verifiable multilateration (VM). In multilateration, the location of a device is precisely computed from a series of known orientation points. The authors have exploited distance bounding and genuine ranging to make sure precise place of a node. Due to the distance bounding usage, an attacking node can quality successful its claimed distance from a situation factor. However, to make positive location consistency, the attacker would additionally need to exhibit that its distance from every other reference factor is shorter. As it isn't usually practicable for the attacker to prove this, it is miles conceivable to come across the attacker. The system is a decentralized range self-governing localization scheme. It's supposed that the locators are relied on and can't be compromised thru any attacker. A sensor calculates its location thru listening to the beacon information sent via all locator that

consists of the locator's region info. The beacon messages are encrypted utilize a shared international symmetric key which is pre-distributed in the sensor nodes. Exploiting the data from

ISSN: 2278-4632
Vol-10 Issue-1 January 2020

eachthe beacons which a sensor node accepts, it calculates it estimated locality rely on the locators coordinates. The sensor node then calculates overlapping antennas are exploiting a majority election scheme. The ultimate sensor node locality is determined via computing the gravity middle of the overlapping antenna area.

F. Time synchronization

The purposes in SN necessitate time synchronization. two Any protection mechanism ought to moreover be time- synchronized. A collaborative WSN can additionally necessitatesynchronization amongst a gathering of sensors. In define a gathering of tightly closed synchronization protocols for multi- hop sender receiver and team synchronization.

G. Authentication

The communicating node is the one that it claims to be. An adversary can't solely alteration statistics packets however additionally can modify a packet move thru inserting fabricated packets. It's, therefore, essential for a receiver to have a mechanism to affirm which the obtained packets have certainly arrive from the real sender node.

VI. SECURITY ISSUES IN WSN

A. Data Integrity

It's very essential in SN to make sure the data consistency. It ensures that data packets that are established through the aim are precisely the ones transfer through the source and any one can't adapt that packet in among.

B. Data Confidentiality

Privacily means to defend data through communiqué in a n/w to be understood other than planned receiver. Cryptography methods are used to offer confidentiality. It's a most important matter in network security.

C. Data Availability

These services are forever accessible in the n/w still in the attack like Dos. Accessibility is of main significance to preserve an operational network.

D. Data Authentication

The statistics familiar through goal has now not been modified at some stage in the transmission. It's reached by means of asymmetric or symmetric mechanisms in which goal and source nodes share secret keys.

E. Data Freshness

The data commonplace via the goal is commonly modernday and fresh information and no challenger can replay the historic info. It's reached via utilising mechanisms as nonce or including timestamp to all data packet [5].

VII. TECHNIQUES TO DEFEND THREATS IN WSN

Security is a mainly utilized time period encompassing aspects of integrity, privacy, authentication, non repudiation and anti- playback. The dangers of the information tightly closed transmission over the n/w increases with amplify in the dependency on the data give thru the network.

A. Encryption

That mechanism offers protection against passive attacks as eavesdropping. SN commonly run in wild or public location overinherently insecure wirelessly channels. It is thereforeinsignificant for a gear to eavesdrop or even add messages into the n/w. The regular key to this issue has been two espouse approach e.g. method symmetric key encryption schemes, public key cryptography and authentication codes.

B. Symmetric encryption

It's additionally recognised as sole one key cryptography. It makes use of a single key. In this encryption manner the goal andthe supply has to approve upon a sole secret (shared) key. Given

ISSN: 2278-4632
Vol-10 Issue-1 January 2020

a message (plain text) and the key, encryptions generate one intelligible records that is regarding the comparable size as the undeniable text was. Decryption is the encryptions reverses, and makes use of the similar key as encryption.

C. Asymmetric encryption

It's additionally recognized as public key cryptography. It uses two keys: public key, which known to the public, used for encryption and private key, which regarded solely to the person of that key, used for decryption. The non-public and public keys are associated with high-quality by any mathematical method. In exclusive words, information encrypted thru a public key can be encrypted only via its constant personal key [6].

D. Cryptography

Electing the most gorgeous cryptographic method is necessary as all security offerings ensure through cryptography in WSNs. Cryptographic technique utilized in WSNs have to meet the sensor nodes constraints and be evaluated through facts size, processing time, and code size [7].

VII. LITERATURE SURVEY

Xiaoliang Meng et al. [2016] in the technique of electing the multi-hop nodes in the WSN, it's substantial to select the subsequent most excellent forwarding node depend on a certain rule. Optimal electing mechanism rely on geographical location data is a protocol which take advantage of distances and angles, as the standards of routing election. TBF protocol confers routing packets along a predefined disperses nodes route as a substitute [8].

Hacène Fouchal et al. [2016] in this paper a dispensed solution able to make sure authentication of nodes at any time without having any online get entry to to a certificates authority. Each node will be device with a Trusted Platform Module (TPM) which is capable to keep keys with security. Each node will have its own public key and private key pair in the TPM and a certificate of the public key. The certificates is issued off-line when setting-up the node. When a node communicates with another, it has to signal the message with its personal personal key (done securely via the TPM) and sends the message, the signature and the certificates of the public key. The assessment of the answer has been whole the use of simulation and the overhead brought through integrating authentication does not exceed 15% of electricity consumption [9].

Gagandeep Kaur et al. [2016] Sensor nodes acquire the data from the surroundings and transmit to BS. But attackers corrupt statistics while transmitting therefore data security is major challenge of WSN. In define protocol; we reduce the passive assault on sink node through lessening the visitors on sink node. The simulation effects demonstrates the outline method can each node will compress their data earlier than sending to clusterhead. After compressing, the packet measurement of node will decrease. This will limit the site visitors overload. In this compression technique, they slash the measurement of packet viadeveloping a code[10].

Janusz Furtak et al. [2016] Ensuring security in the navy utilization of IoT is a largest challenge. The predominant motives for this affairs kingdom is that the sensor nodes of the n/w are normally mobile, use wirelessly links, have a small processing energy and have a little power resources. The paper defines the answer for cryptographic safety of transmission between sensors nodes in the information hyperlink layer and for cryptographic safety of records save in the sensor node resources. The TPM used to be utilized. The define result makes it possible to build tightly closed and fault tolerant SN. The following aspects have been presented in the paper: the mannequin of such a network, utilized safety solutions, studies of the safety in the n/w and elected investigation effects of such a community were [11]

Mauricio Tellez et al. [2016] with the quickly technological progressions of sensors, WSNs have grow to be a typical technological know-how for the IoT. They examined the WSNs safety

ISSN: 2278-4632
Vol-10 Issue-1 January 2020

In an environment monitoring utilization with a goal to show the overall security. They applied a STMS, that served as our WSN usage. Our effects revealed a safety flaw located in the bootstrap loader (BSL) password utilized to guard MSP430 micro-controller units (MCUs). They illustrate how the BSL password can be brute pressured in a depend of days. Furthermore, we illustrate how an attacker can reverse engineer WSN functions to gain critical security information such as encryption keys. We make a contribution a answer to patch the susceptible BSL password protection flaw and better the protection of MSP430 MCU chips. The Secure-BSL patch we make a contribution permits the randomization of the BSL password. Our end result rises the brute force time to decades. The unusable brute pressure time accompaniments the security of the MSP430 and averts future reverse engineering devices. Our research serves as proof that the security of WSNs and the standard IoT technology is broken if we can't shield these every day objects at the bodily layer [12]

Pooja M.Shukre et al. [2016] Security and confidentiality of statistics is very tons critical whilst deploying a WSN. Depending on the surroundings in which network is deployed; configuration parameters of network nodes want to be updated time to time. This can be reached take advantage of dissemination protocols and statistics discovery. DiDrip is the preliminary dissemination protocol and records discovery that has been designed through taking distinct safety vulnerabilities in think. The protocol expedites community proprietor to permit a couple of community customers having distinctive privileges for simultaneous and direct dissemination of records into the n/w nodes. This paper outline a new technique to minimalize packet loss throughout data dissemination the use of DiDrip protocol and grant excessive safety to WSN. RSA and Diffie Hellman key trade algorithm are used as methods of encryption [13].
Muhammad Umar Aftab et al. [2015] this paper defines the sorts of WSNs and the likely results for tackling the listed difficulties and consequences of many different issues. This paper will transport the data related to the WSN and shape with literature assessment so that a person can get greater information concerning this emerging area [14].

Biji Nair et al. [2015] the purposes range rely on WSN is extensive. Security result implementation is a important hassle as these networks are shaped from useful resource constrained tiny sensor nodes which have meager computational energy and community lifetime. Moreover, the purposes necessitate numerous section of security. A wellknown safety solution isn't possible in such networks. ECC is emerging like a promising protection end result for WSN. Certain functions that require primary protection degree need no longer be careworn with the aid of the use of trendy safety measures which may additionally tax on their efficiency. The correct selection of values of Elliptic Curves (EC) parameters is of paramount significance whilst imposing ECC for resource confined WSN. This paper identifies the relevant parameters of EC for ECC implementation in WSN and analyses the impact in their values on the extent of safety they provide [15].

CONCLUSION

WSN are networks which are comprised of sensors that are distributed in an advert hoc way. WSNs are turning into a costeffective, sensible way to go about deploying sensor networks .we use the greedy algorithm and grid-based technology. The scheme is additionally able to keep away from the voids and limitations in the community by means of its decentralized forwarding technique, thereby decreasing packet drop due to community load, As against the compared approach. The outcomes exhibit that GBRR successfully identifies the redundant nodes and agenda them on the other hand in the surroundings with random obstacles. All these make GBRR reliable scheme that has the potential to enhance the typical network nice of carrier for WSN.

I. REFERENCES

[1] NM. Nair, JS. Terence, "*Survey On Distributed Data Storage Schemes In Wireless Sensor*

ISSN: 2278-4632
Vol-10 Issue-1 January 2020

Networks", Indian Journal of Computer Science and Engineering (IJCSE), Vol.4, No.6, pp.1-6, 2014.

[2] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "*Wireless sensor network survey*", Science direct, Vol.52, Issue.12, pp.2292– 2330, 2008.

[3] AS. Mandloi, V. Choudhary, "*An Efficient Clustering Technique for Deterministically Deployed Wireless Sensor Networks*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.1, pp.6-10, 2013.

[4] Sanchita Gupta, Pooja Saini, "*Modified Pairwise Key Pre- distribution Scheme with Deployment Knowledge in Wireless Sensor Network*", International Journal of Scientific Research in Network Security and Communication, Vol.1, Issue.2, pp.21-23, 2013.

[5] N. Meenaksi, P. Rodrigues, "*Tsunami Detection and forewarning system using Wireless Sensor Network - a Survey*", International Journal of Computer Sciences and Engineering, Vol.2, Issue.3, pp.76-79, 2014.

[6] Chanchal Yadav, SS. Hegde, NC. Anjana, Sandeep Kumar, "*Security Techniques in Wireless Sensor Networks : A Survey*", International Journal of Advanced Research in Computer and Communication Engineering, Vol.4, Issue.4, pp.289-295, 2015.

[7] Jaydip Sen, "*A Survey on Wireless Sensor Network Security*", International Journal of Communication Networks and Information Security, Vol.1, No.2, pp.1-16, 2009.

[8] Xiaoliang Menga, Xiaochuan Shia, Zi Wangb, Shuang Wua, Chenglin Lia, "*A grid-based reliable routing protocol for wireless sensor networks with randomly distributed clusters*",elsevier, Vol.51, NO.11, pp.47–61, 2016.

[9] Hacene fouchal, javier biesa, elena romero, alvaro araujo, octavio nieto taladrez, "*a security scheme for wireless sensor networks*", 2016 IEEE Global Communications Conference (GLOBECOM), Washington, pp.1-5,2016.

Gagandeep Kaur, Deepali, Rekha Kalra,"*Improvement andanalys security of WSN from passive attack*", 2016 5th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), Noida, pp.420-425, 2016